APPENDIX B

Windows Wireless Architecture

Tim Moore
Lead Program Manager
Windows Networking
Microsoft Corporation

Agenda

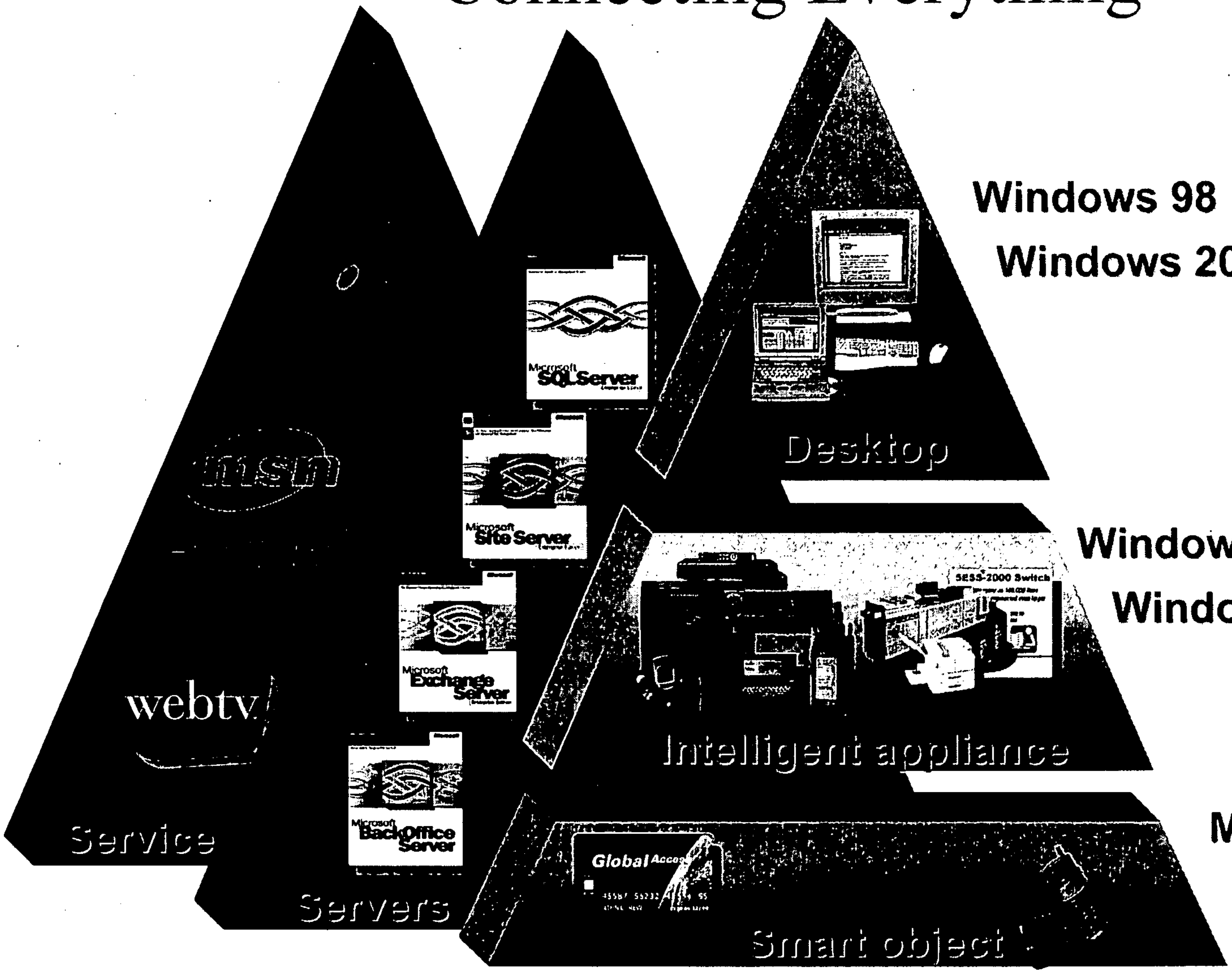
- Wireless trends
  - WAN, LAN, PAN
- Scenarios
  - Adhoc, home, small business
  - Enterprise, ISP
- Wireless architecture
- Summary
- Call to action
- More information

Wireless Trends

- IP networks
- Always connected
- Increased bandwidth
- Convenience
- Moving from vertical market to horizontal markets
- Moving from proprietary to standards based
- Proliferation of smart devices
- New scenarios enabled
- Outsourcing
- Adhoc networks

Information Anytime, Anywhere

Connecting Everything



Windows 98
Windows 2000

Windows NT Embedded
Windows CE

Micro-browser
Smart Card for
Windows

Data Speeds Today

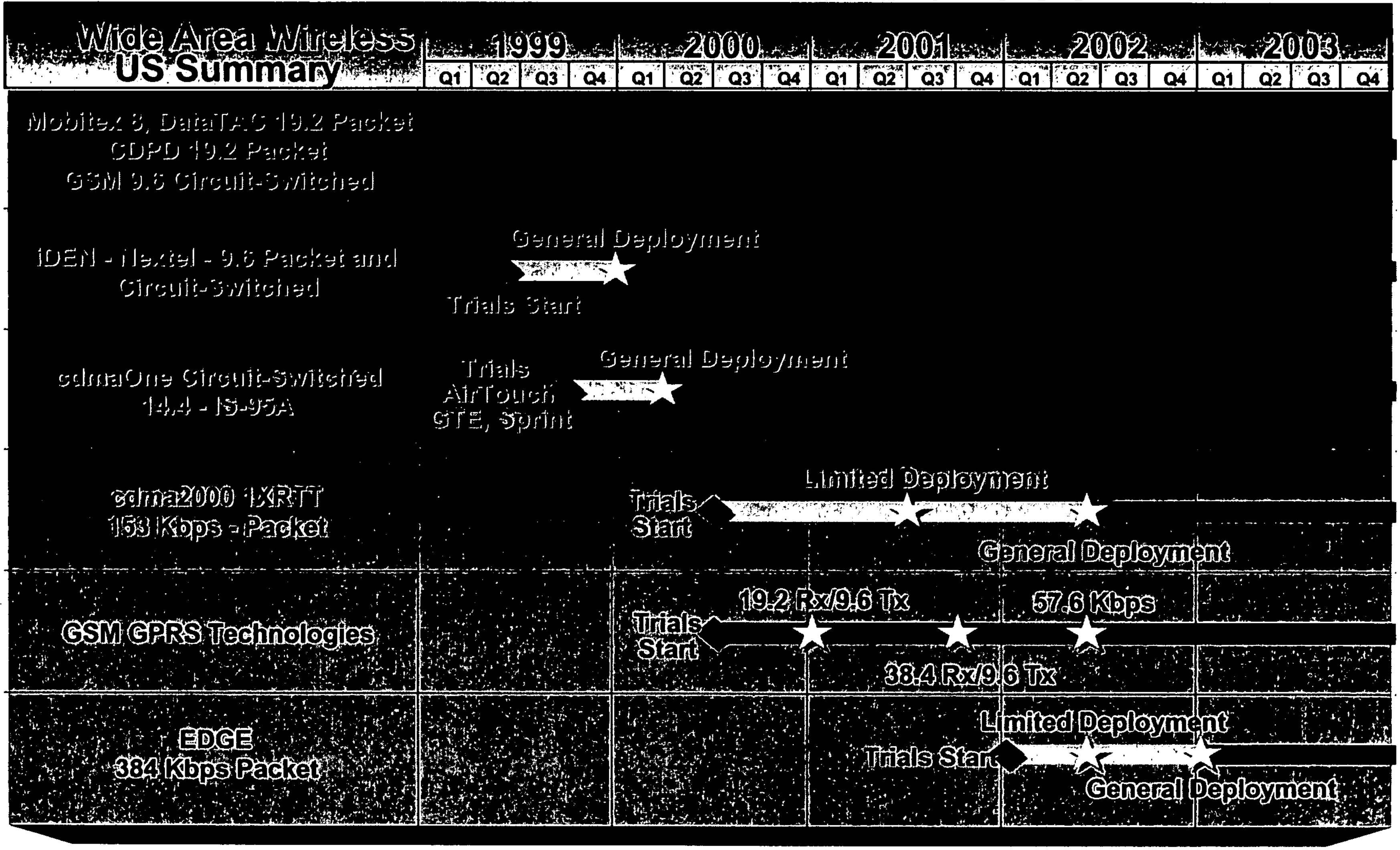
Network	Speed	Type of Data
[illegible]	[illegible]	[illegible]
CDMA	14.4 Kbps	Circuit-Switched
Nextel	9.6 Kbps	Circuit-switched
GSM	9.6 Kbps	Circuit-Switched
Metricom	28.8 Kbps	Packet as Dial-up
TDMA**	One-Way SMS Only	None

*Typical data throughput speed is usually 50% of gross speed

**TDMA systems do not support data in the U.S. at this time

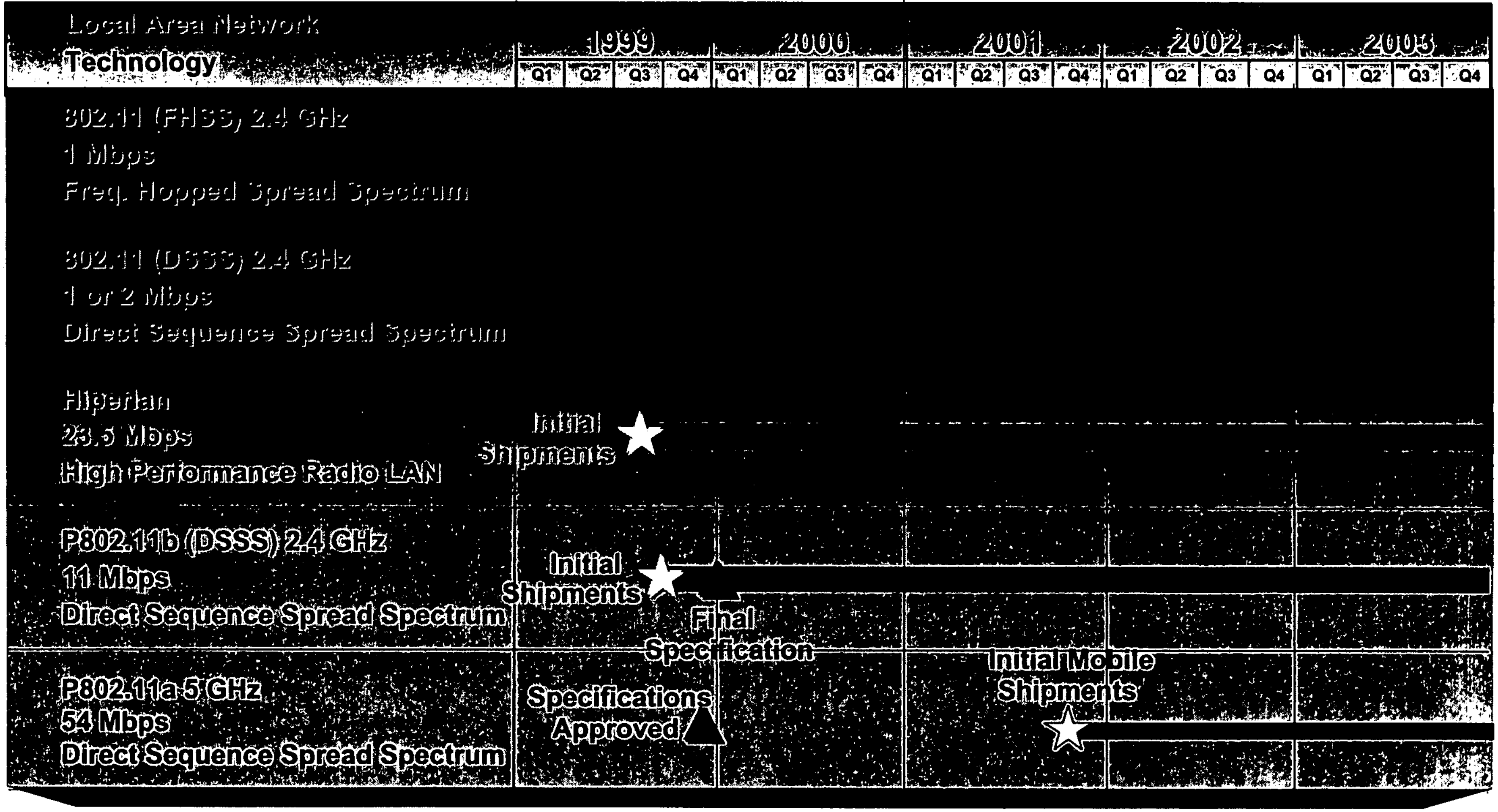
Materials from Andrew Seybold-Microsoft Exchange Conference 1999

Wide-Area Wireless



Materials from Andrew Seybold-Microsoft Exchange Conference 1999

Local-Area Wireless



Local Area Network Technology

1999 Q1 Q2 Q3 Q4 | 2000 Q1 Q2 Q3 Q4 | 2001 Q1 Q2 Q3 Q4 | 2002 Q1 Q2 Q3 Q4 | 2003 Q1 Q2 Q3 Q4

802.11 (FHSS) 2.4 GHz
1 Mbps
Freq. Hopped Spread Spectrum

802.11 (DSSS) 2.4 GHz
1 or 2 Mbps
Direct Sequence Spread Spectrum

Hiperlan
23.5 Mbps
High Performance Radio LAN

Initial Shipments

P802.11b (DSSS) 2.4 GHz
11 Mbps
Direct Sequence Spread Spectrum

Initial Shipments

Final Specification

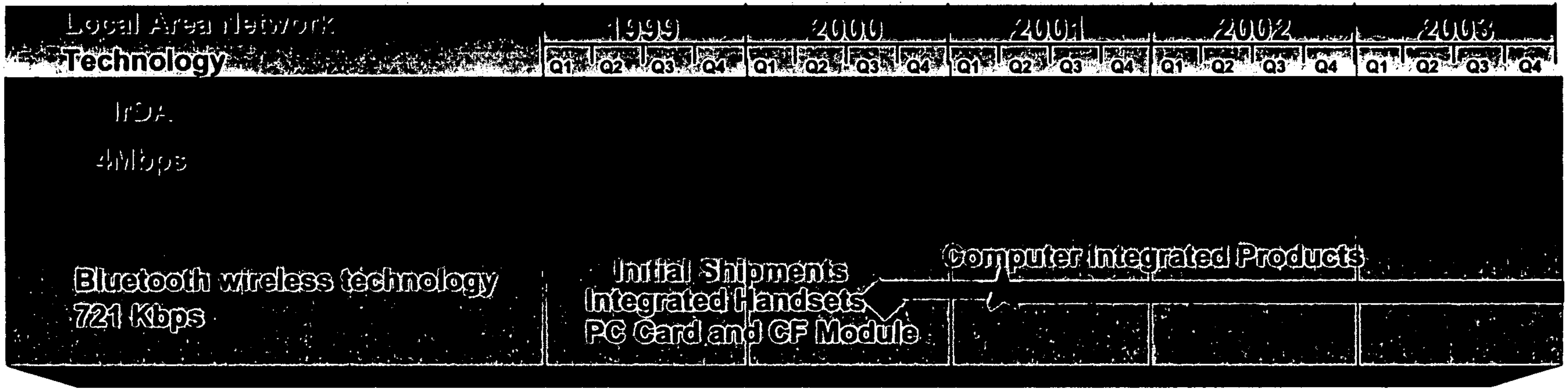
P802.11a 5 GHz
54 Mbps
Direct Sequence Spread Spectrum

Specifications Approved

Initial Mobile Shipments

Materials from Andrew Seybold-Microsoft Exchange Conference 1999

Personal Area Wireless



Materials from Andrew Seybold-Microsoft Exchange Conference 1999

Personal Area Wireless

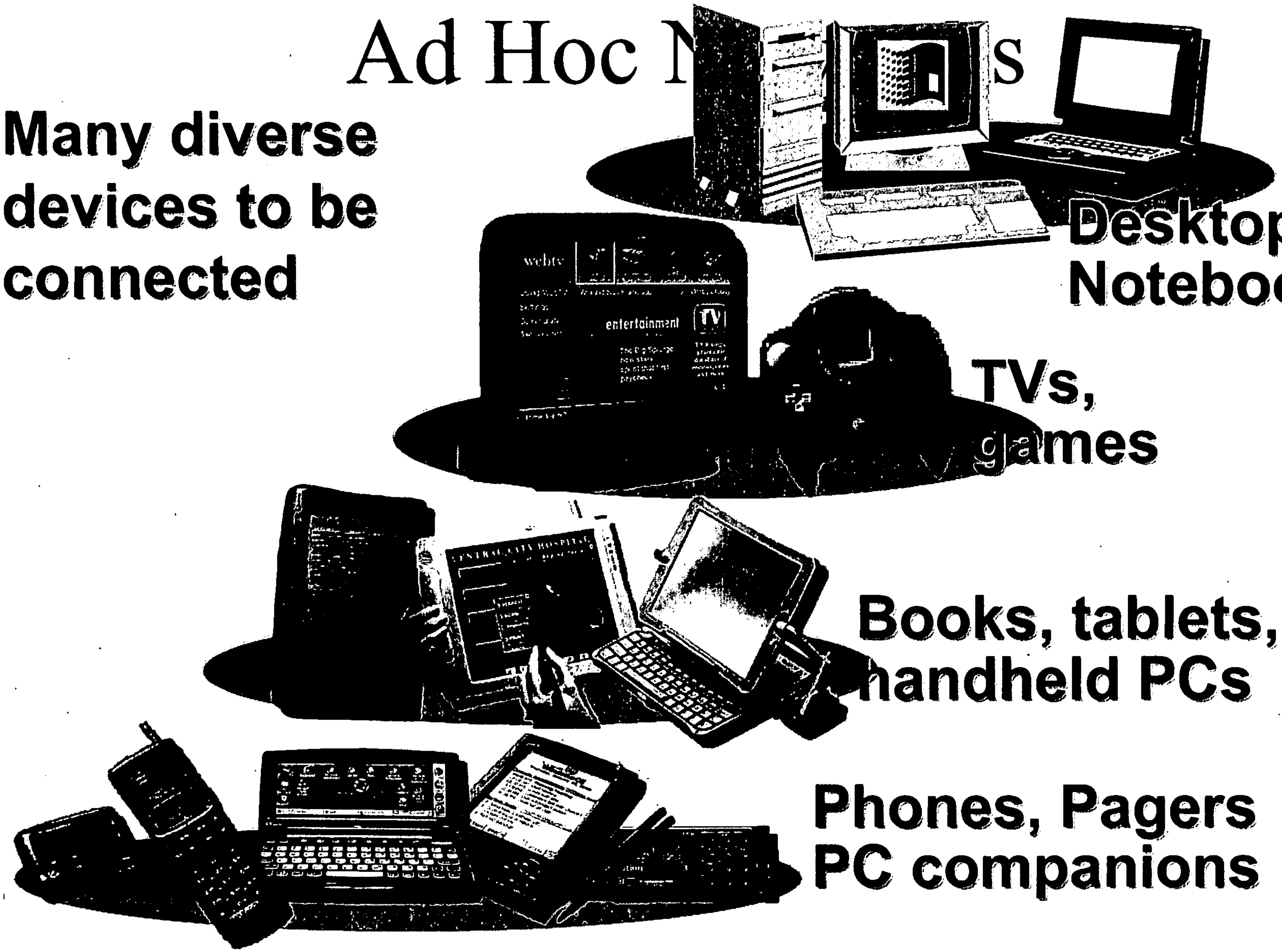
- IrDA
  - Around since 1994
  - Available on every PC and lots of devices
    - >20 million existing IrDA devices
    - Camera, PDAs, cellphones, printers, keyboards
- Exploding market fueled by Bluetooth momentum
  - Bluetooth wireless technology is a defacto standard
  - Proliferation of smart devices, convenience of cable replacement, and new usage scenarios

Scenarios

- Adhoc
- Home
- Small business
- Enterprise
- ISP

Ad Hoc N s

- Many diverse devices to be connected
-



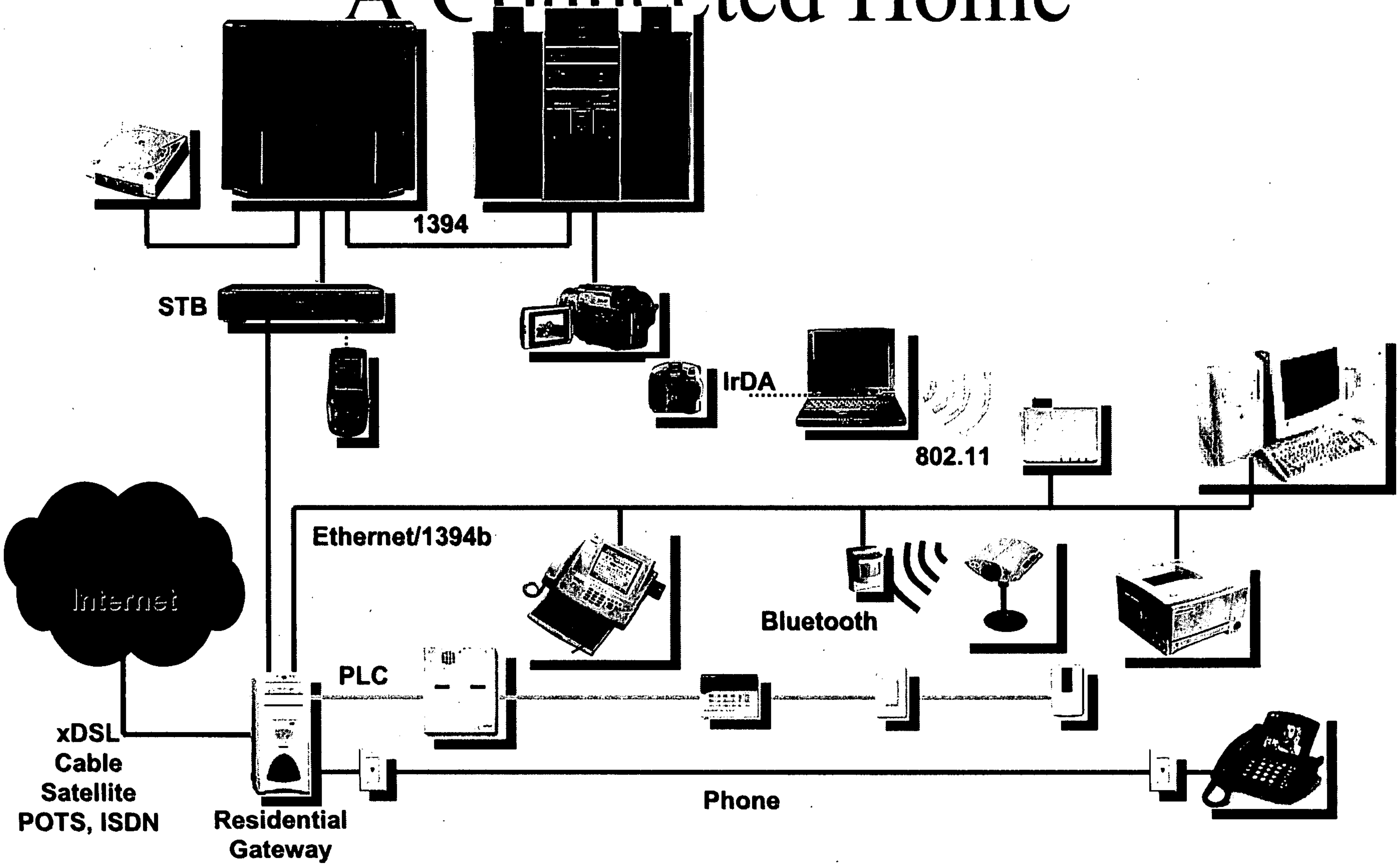
Desktops, Notebooks

TVs, games

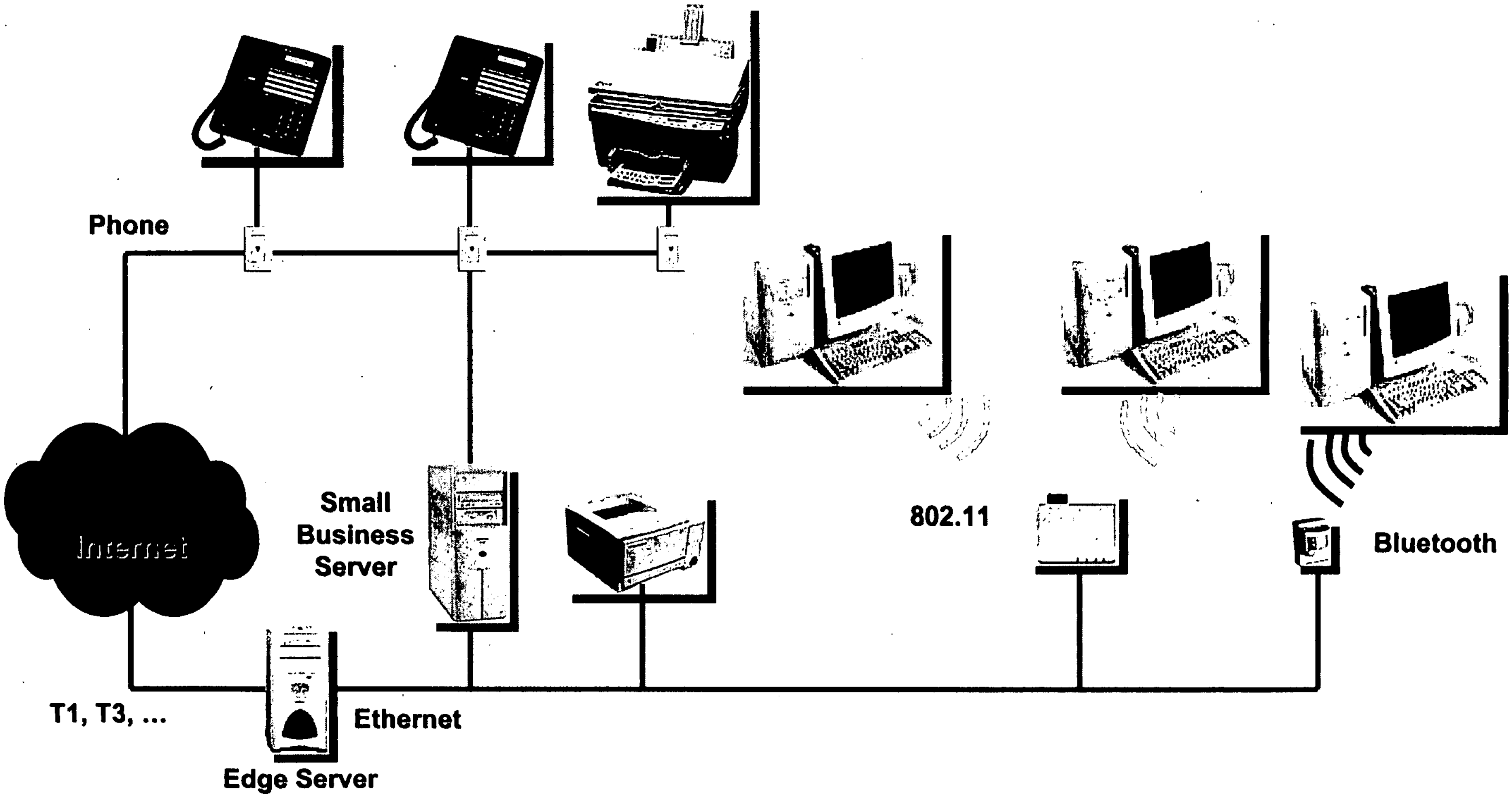
Books, tablets, handheld PCs

Phones, Pagers PC companions

A Connected Home

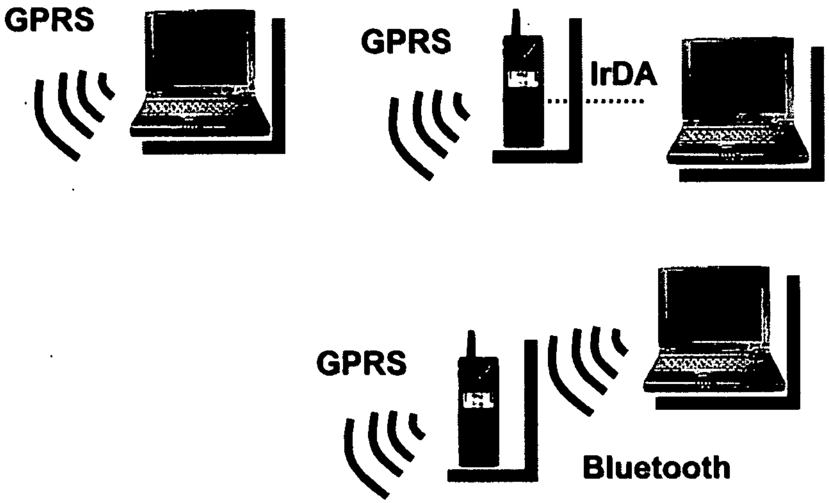


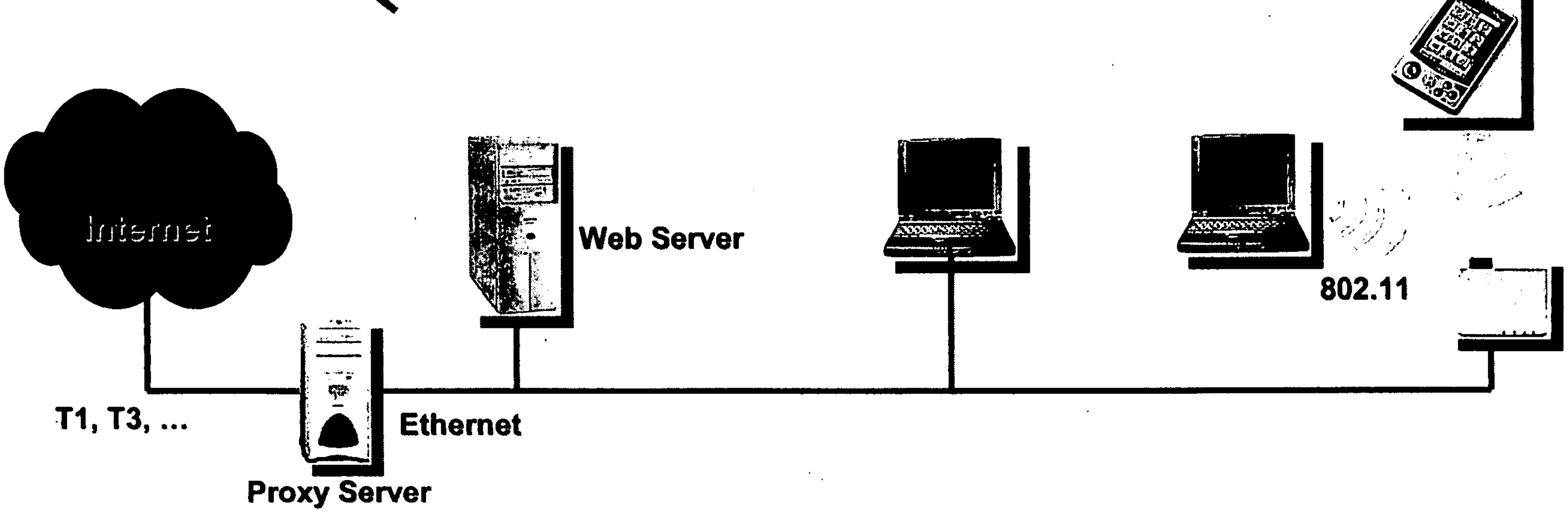
A Connected Small Office



Enterprise

- Information at your fingertips
  - At meetings, in the office, on the road
  - Reliable, secure, multimedia LAN



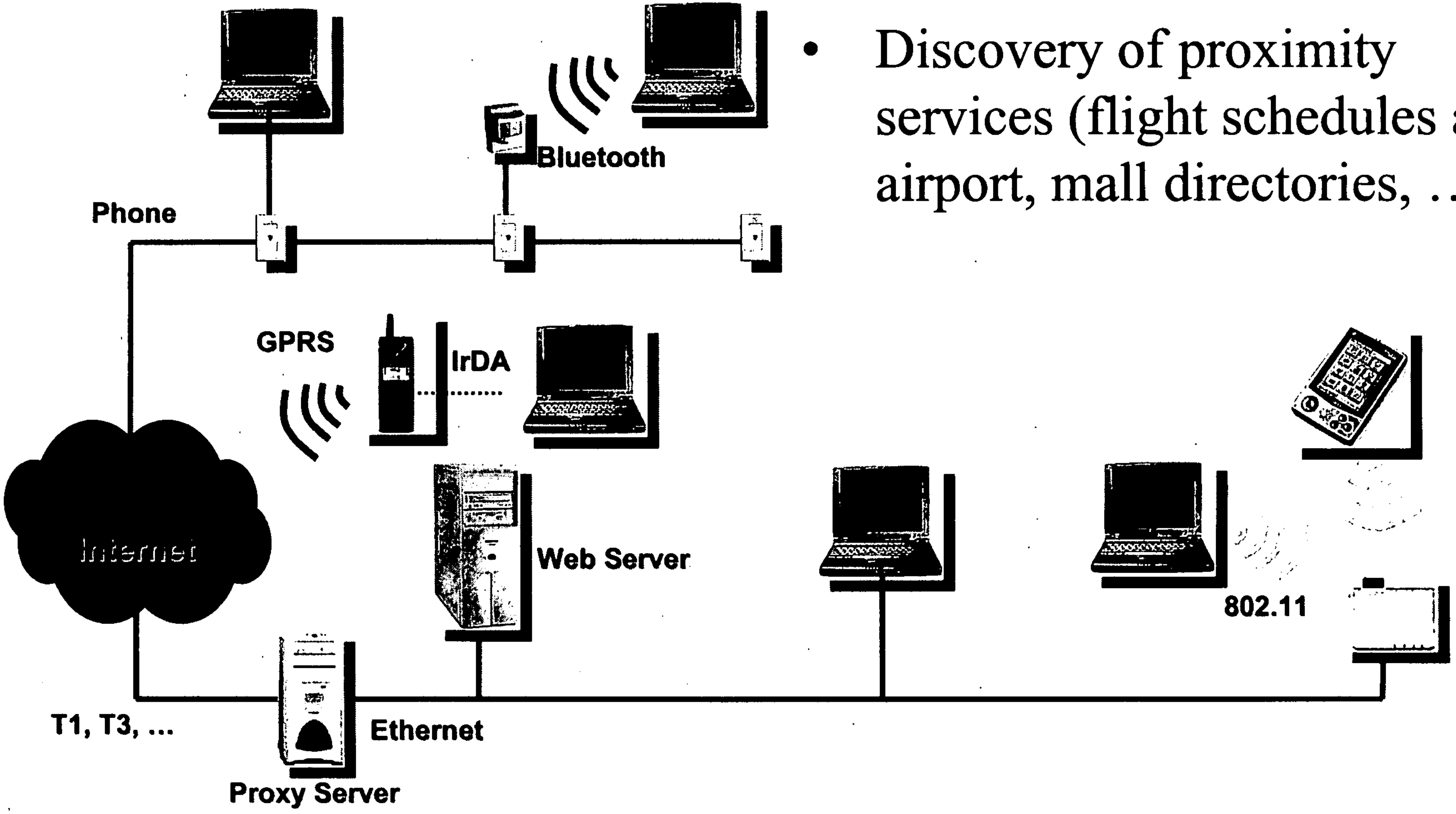


Enterprise

- End-user can access the enterprise wireless network transparently over a secure connection
  - The network administrator has control over which users have access to the enterprise wireless LAN
- Enterprise can offer its employees access via ISPs which outsource their authentication to the enterprise
  - End-user has IP connectivity as soon as a CDPD or a GPRS modem is plugged in
  - Make cellphones an always connected Internet access point using GPRS
- End-User can use Netmeeting with wireless LAN, when out of range of LAN can continue to conference via IP connected cellphone

An ISP Connected Public Space

- Discovery of proximity services (flight schedules at airport, mall directories, …)



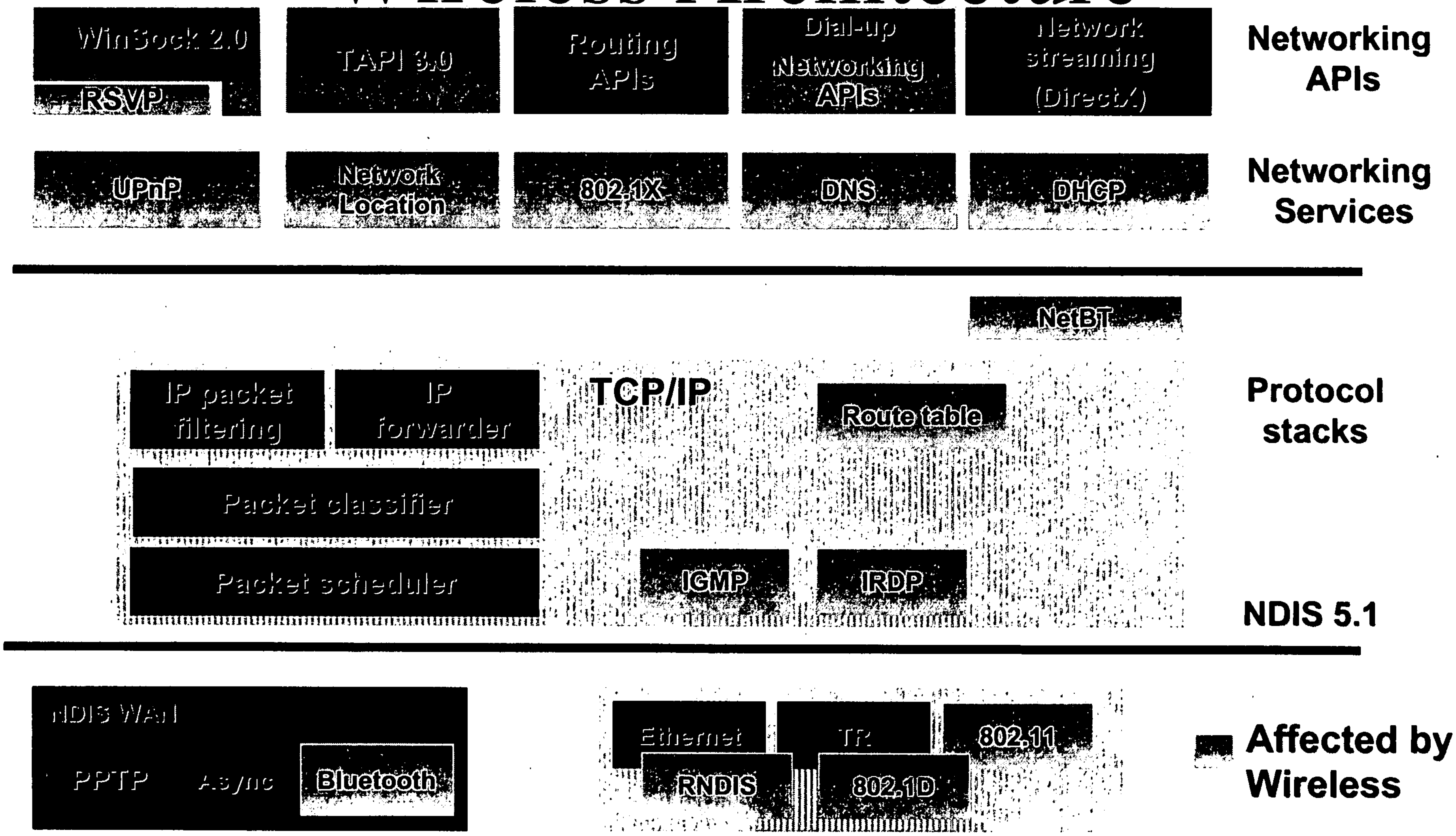
ISP

- Need mixed technologies
  - Higher speed in hot spots, e.g., 802.11
- Need authentication so ISPs can charge
- Allow ISPs to integrate into existing Radius systems
  - Allows ISP roaming agreements
    - Same as outsource dial
- Need to be able to provision unauthenticated users

Wireless Architecture

- "Just works"
- Always connected
- Unified transport: IP
- Mobility
- Unified security model
- Adhoc
- QoS
- Performance

Wireless Architecture



Just Works

- No configuration
  - Especially when roaming
- CDPD
  - Configure Network Equipment Identifier
- 802.11
  - Configure network name and security keys
    - Per location
- Bluetooth wireless technology
  - Configure PIN numbers
    - Per device

802.11 Configuration

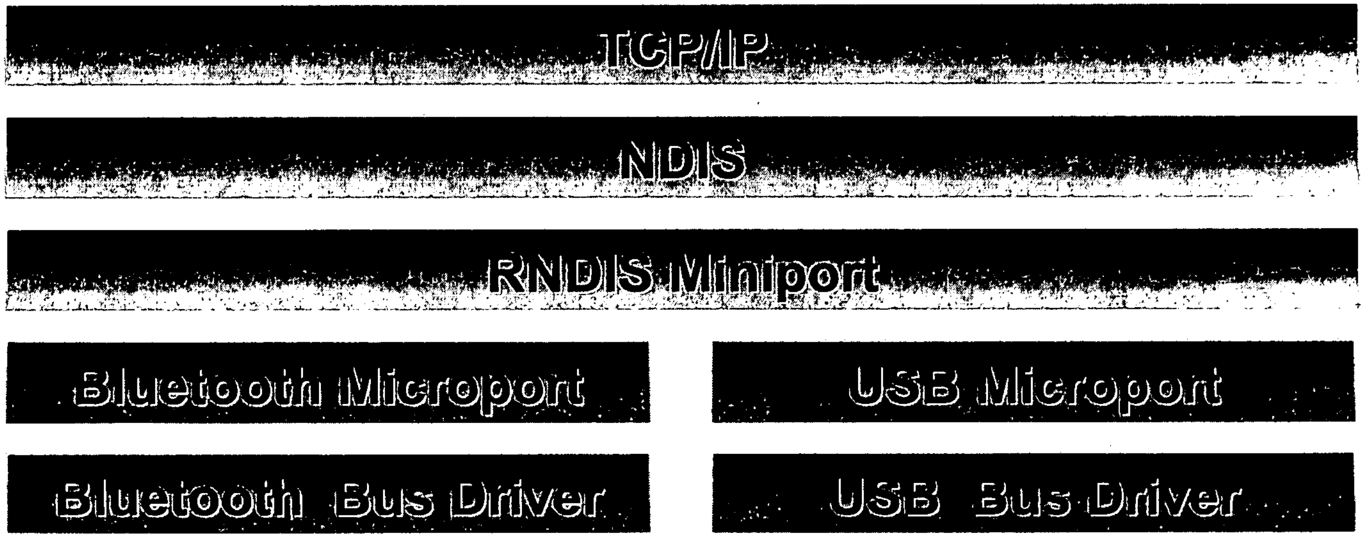
- Current 802.11 networks need to be configured with name of the network
  - Roaming between multiple networks difficult especially when security is implemented
- Automatically find a wireless network
  - If Access point is beaconing network name, attempt to use that network
  - If no infrastructure available then switch to adhoc mode

Always Connected

- Permanent IP connectivity should not use dial-up model
  - A CDPD card should appears as a LAN card
  - A GPRS, EDGE or 3G card or cellphone should appear as a LAN card
    - GPRS Terminal Type Recommendations
      - Cellphone needs to be Type A (voice and packet)
      - PC-Card can be Type C (packet only)
- Implement an NDIS driver or use Remote NDIS
  - Remote NDIS over Bluetooth connections

Remote NDIS

- Remote NDIS enables a bus-agnostic connection to devices that provide network access
- Remote NDIS is both a driver architecture and a command language



TCP/IP

NDIS

RNDIS Miniport

Bluetooth Microport

USB Microport

Bluetooth Bus Driver

USB Bus Driver

Unified Transport: IP

- All other media except Bluetooth wireless technology support always connected IP
- Ethernet over point-to-point Bluetooth connections
  - L2 bridge gives an adhoc L2 network
- Adhoc applications use UPnP over IP
- Expect large numbers of wireless connected devices
  - Move to IPv6 for addresses

Mobility

- Applications should not rely on having a network available all the time
  - Network connection can disappear at anytime
  - Applications should reconnect automatically if the network appears
- Clients hold state about the network
  - IP address
  - Routes
- Networks hold state about the client
  - Multicast distribution
  - Quality of service
  - Secure access
  - Machine name to IP address mapping
- How to detect when this state is out of date
- Applications also hold state about the network
  - TCP connections
  - E.g. Proxies, firewalls, etc.

Mobility

- Detect roaming
  - Mediasense detects working/non-working interfaces
  - Mediasense detects interfaces changing their network connection
- IP address
  - Mediasense triggers a DHCP renew; If renew fails, DHCP gets a new IP address
  - DHCP updates DNS when an address changes
  - TCP/IP removes IP addresses if NIC not connected
  - Mobile IP allows IP address to stay the same when roaming

Mobile IP

- Mobile IP keeps the application IP address the same
  - IPv4 has two options
    - Change the network interface address to a local IP address
    - Use an ARP proxy to keep the same IP address
  - IPv6 only has first option
- Mobile IP Issues
  - How to route efficiently
    - IPv6 fixes this issue
  - Firewall traversal
  - Time to get a local address
    - Doesn’t allow Voice over IP roaming
- Doesn’t address any of the other issues with multicast, QoS, security, applications
- GPRS and 3G have network layer mobility
- No plans to support Mobile IP until IPv6

Mobility

- Multicast
  - Mediasense triggers IGMP refresh on roaming
- QoS
  - Mediasense triggers RSVP refresh on roaming
- Routes
  - Mediasense triggers router detect (IRDP) on roaming
  - Default interface metrics should depend interface speed
  - Routes to no longer existing interface addresses are removed
- Security
  - Mediasense triggers network authentication refresh
- Applications
  - Need to retry connections on connection failure and mediasense
  - Configurations based on network location

Network Location API

- Network location is a hint to the application of the network the machine is connected to
- Accessible via Winsock API
  - Query for the connected networks
    - WSALookupServiceBegin
    - WSALookupServiceNext
    - WSALookupServiceEnd
  - Request for notification when the connected networks changes
    - WSANSIoctl (,SIO_NSP_NOTIFY_CHANGE,…)
- Applications that need configuration per network should use this API
  - E.g., application proxies

Security

- Secure access to resources in the network
  - This is Windows login
- Secure transfer of data over the network
  - This is IPSec
  - Integrated into Windows credentials using PKI and Kerberos
- Secure access to the network
  - This is available for RAS and VPNs
  - Integrated into Windows credentials using PKI (EAP) and Radius
  - Supports roaming of identities
- No secure access to LAN networks
  - Very important for Wireless

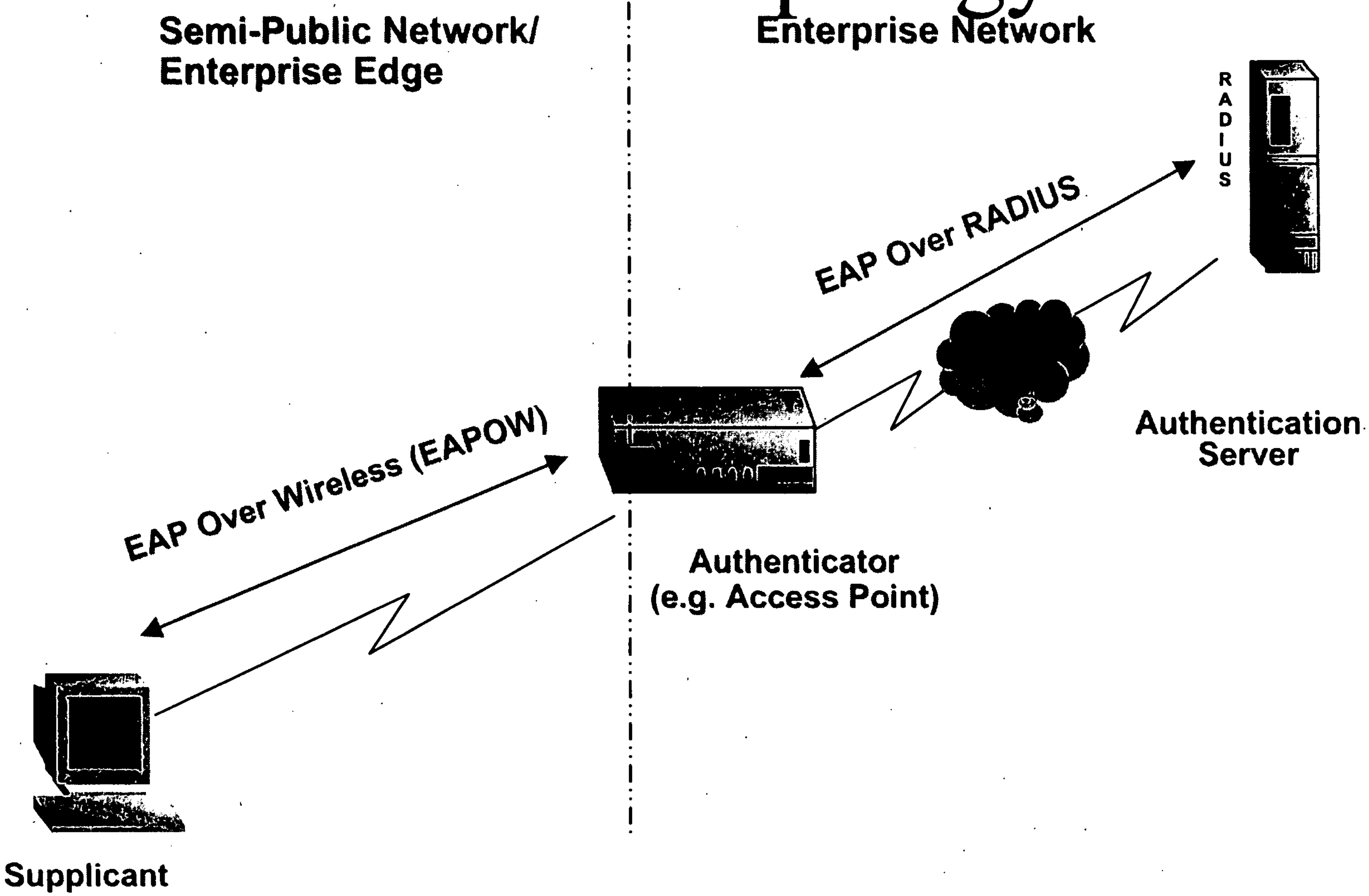
Wireless Security Issues

- User loses wireless NIC, doesn’t report it
  - Without user authentication, Intranet now accessible by attackers
  - Without centralized accounting and auditing, no means to detect unusual activity
    - Users who don’t log on for periods of time
    - Users who transfer too much data, stay on too long
    - Multiple simultaneous logins
    - Logins from the “wrong” machine account
  - With global keys, large scale re-keying required

Wireless Deployment Issues

- User administration
  - Integration with existing user administration tools required (RADIUS, LDAP-based directories)
    - Create a Windows group for wireless
    - Any user or machine who is a member of the group has wireless access
  - Identification via User-Name easier to administer than MAC address identification
  - Usage accounting and auditing desirable
- Key management
  - Static keys difficult to manage on clients, access points
  - Proprietary key management solutions require separate user databases

802.1X Topology



Semi-Public Network/
Enterprise Edge

Enterprise Network

RADIUS

EAP Over RADIUS

Authentication Server

EAP Over Wireless (EAPOW)

Authenticator
(e.g. Access Point)

Supplicant

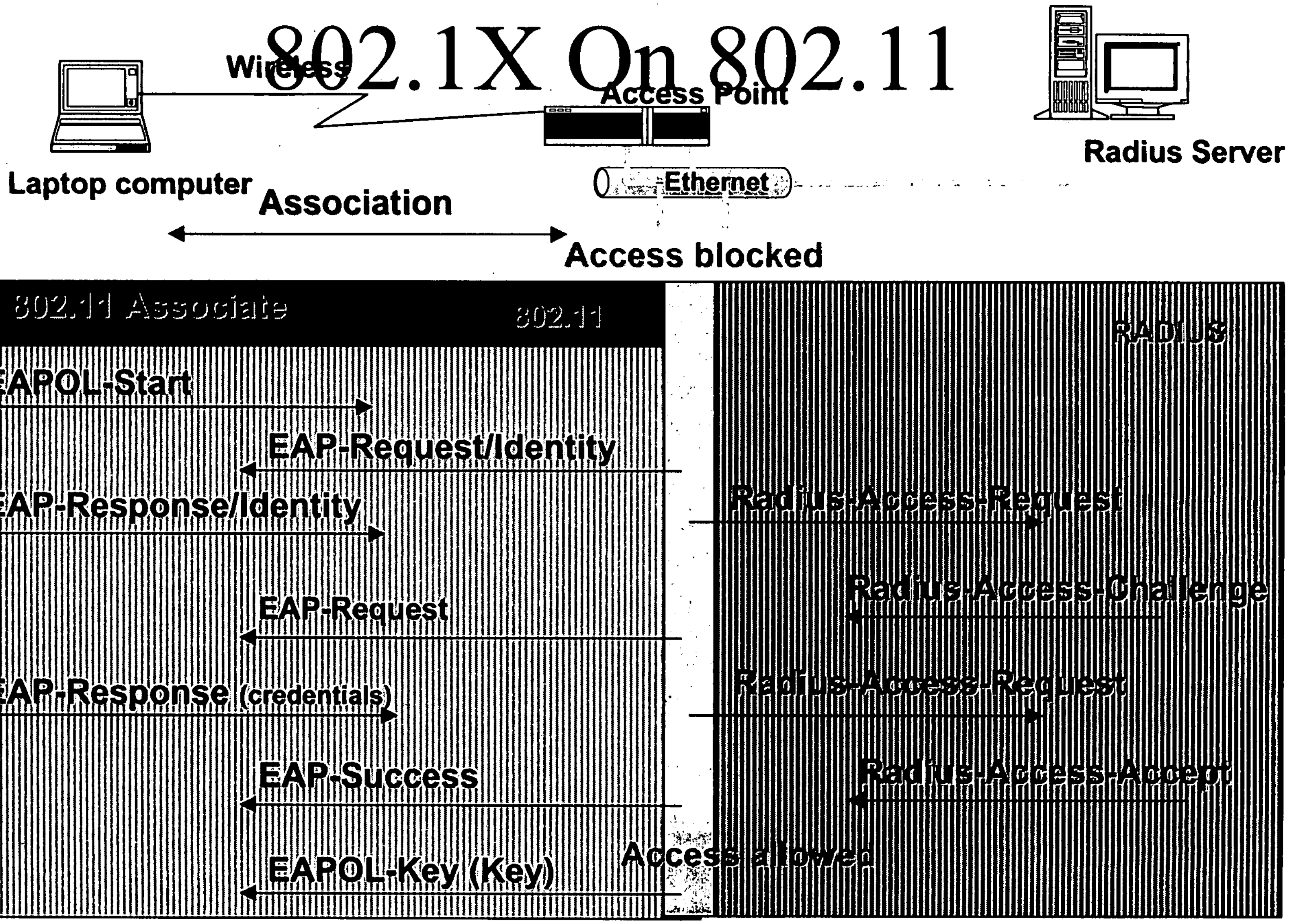
IEEE 802.1X

- Enables interoperable user identification, centralized authentication, key management
  - Leverages existing standards: EAP, RADIUS
  - Compatible with existing roaming technologies, enabling use in hotels and public places
- User-based identification
  - Identification based on Network Access Identifier (RFC 2486) enables support for roaming access in public spaces (RFC 2607)
- Dynamic key management
- Centralized user administration
  - Support for RADIUS (RFC 2138, 2139) enables centralized authentication, authorization and accounting
  - RADIUS/EAP (draft-ietf-radius-ext-07.txt) enables encapsulation of EAP packets within RADIUS
- Supported on Ethernet, Token Ring and 802.11

Extensible Authentication Protocol

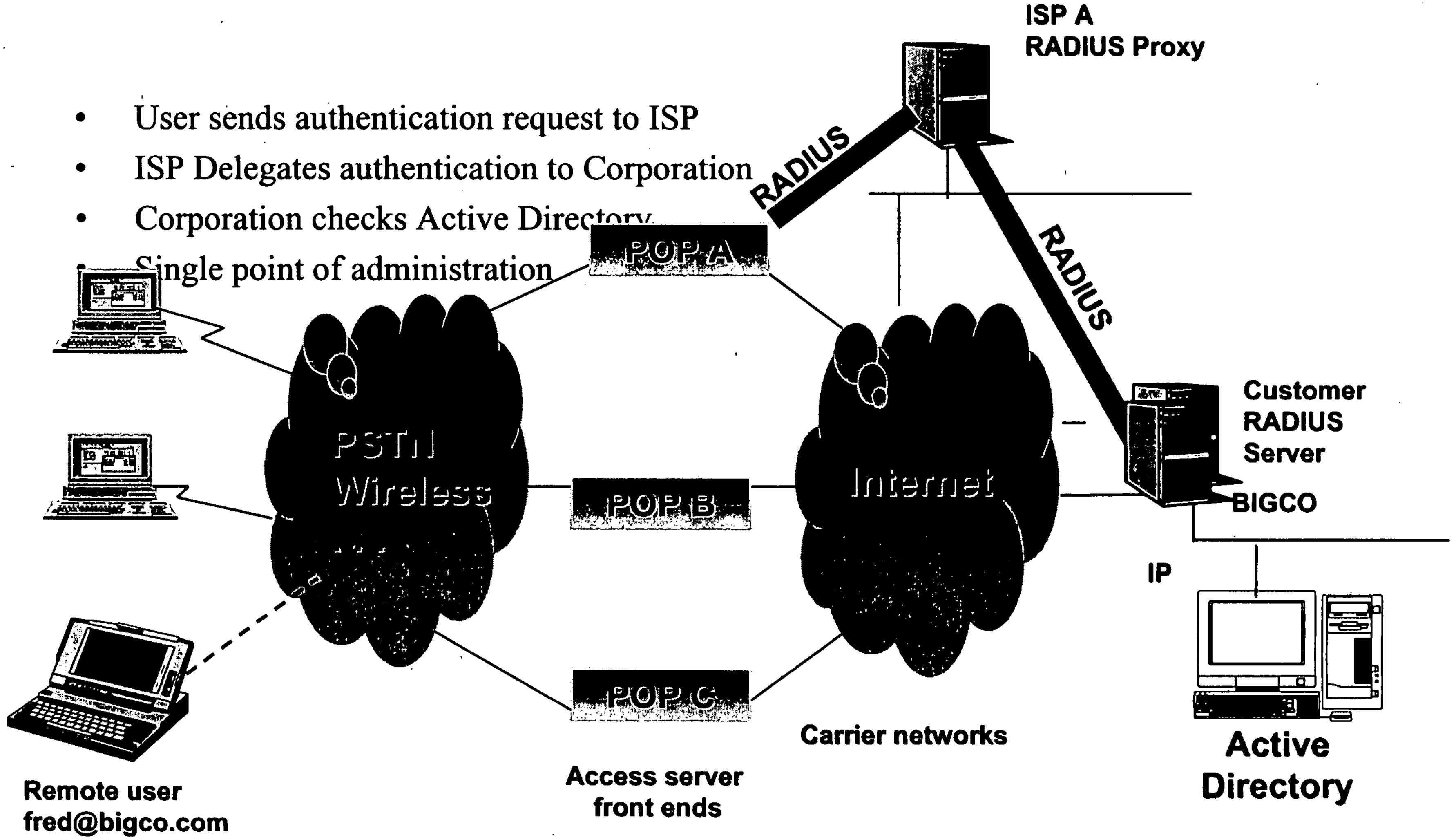
- Used by PPP for RAS and VPN
- Allows support for a number of authentication mechanisms
  - EAP designed to allow additional authentication methods to be deployed with no changes to the access point or client NIC
  - RFC 2284 includes support for password authentication (EAP-MD5), One-Time Passwords (OTP)
  - Windows 2000 supports smartcard authentication (RFC 2716) and Security Dynamics
- Radius server used for authentication and authorization
  - Integrated into Active Directory™ users and groups
  - Supports cross authentication for roaming

802.1X On 802.11

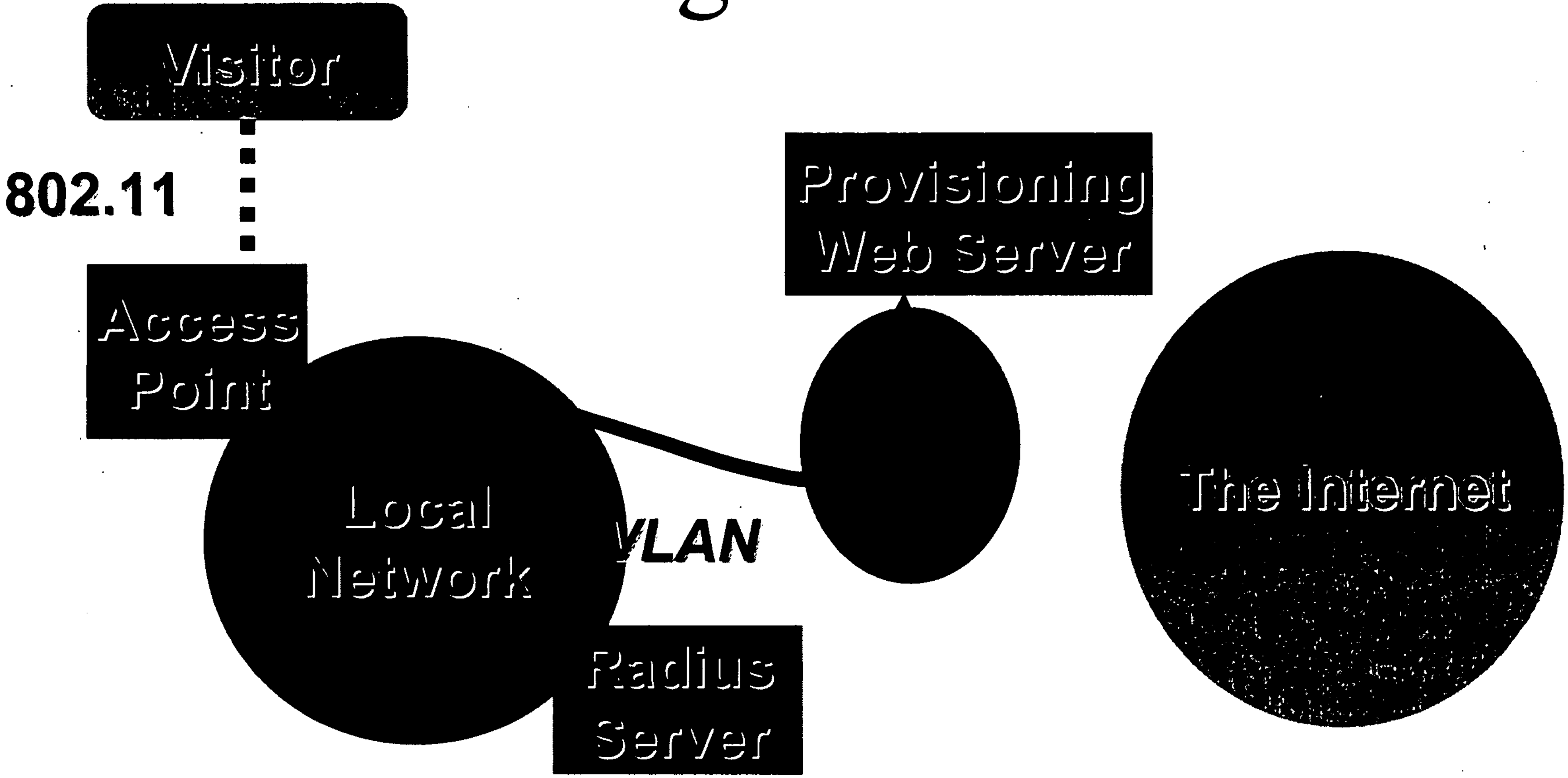


Outsourced Remote Access

- User sends authentication request to ISP
- ISP Delegates authentication to Corporation
- Corporation checks Active Directory
- Single point of administration



Provisioning Public Internet



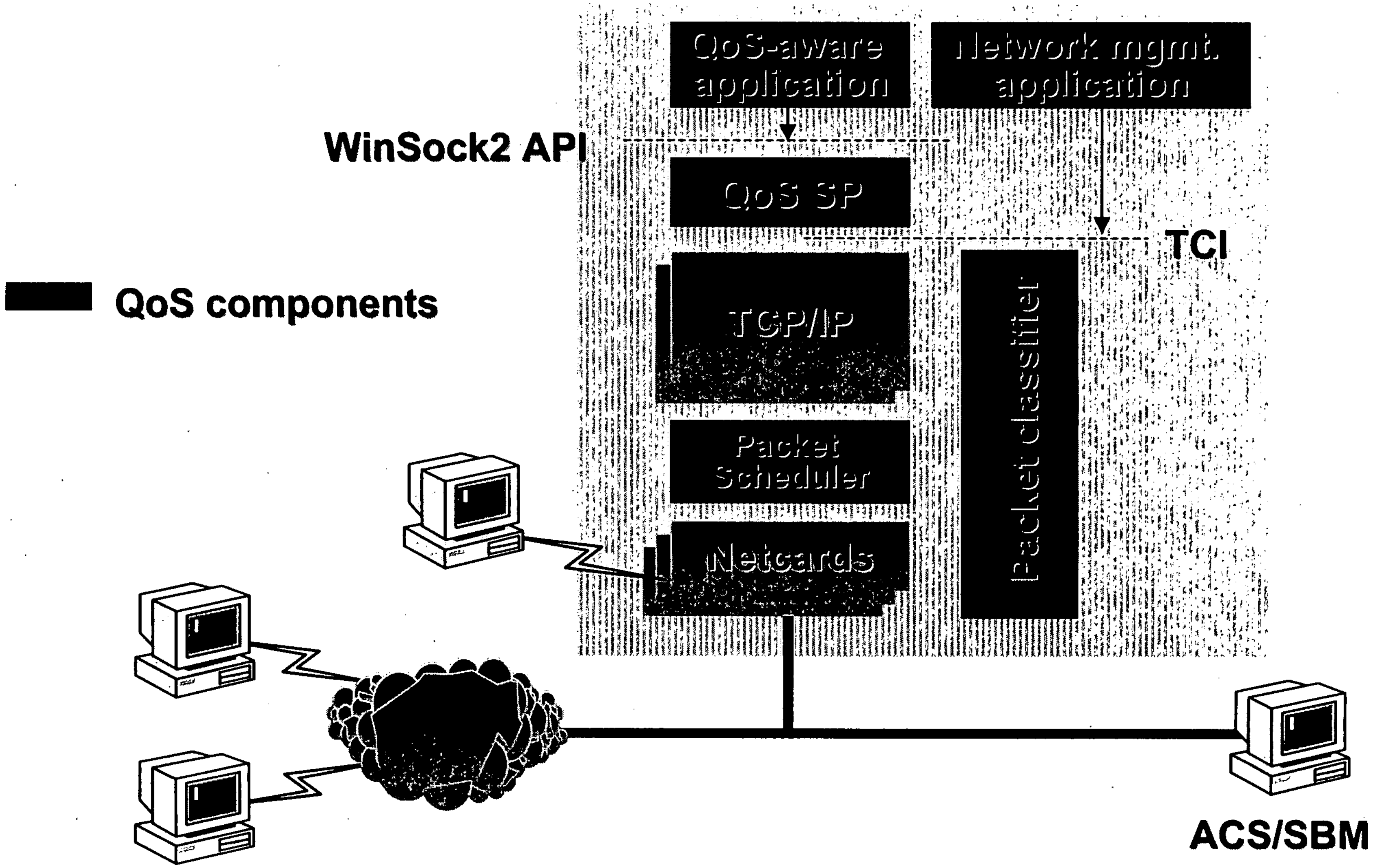
Bluetooth Security

- To connect to a Bluetooth device requires its PIN
- PIN is per device not per service
  - Great for personal single function devices
  - E.g., protect cellphone from being dialed
- Problem for adhoc devices/applications
  - Require PIN for each device
  - Obtain access to all services on device
- Need security at a higher level and no PIN
  - Adhoc FTP user intervention required so why need a pin?
  - Adhoc PAN do not want a PIN otherwise cannot setup roaming PANs
  - Business card exchange should be push to a destination

GPRS Security

- GPRS uses GSM Authentication
- Authentication is between the mobile station and the network
  - Need authentication between PC and the Bluetooth mobile station
    - Bluetooth PIN

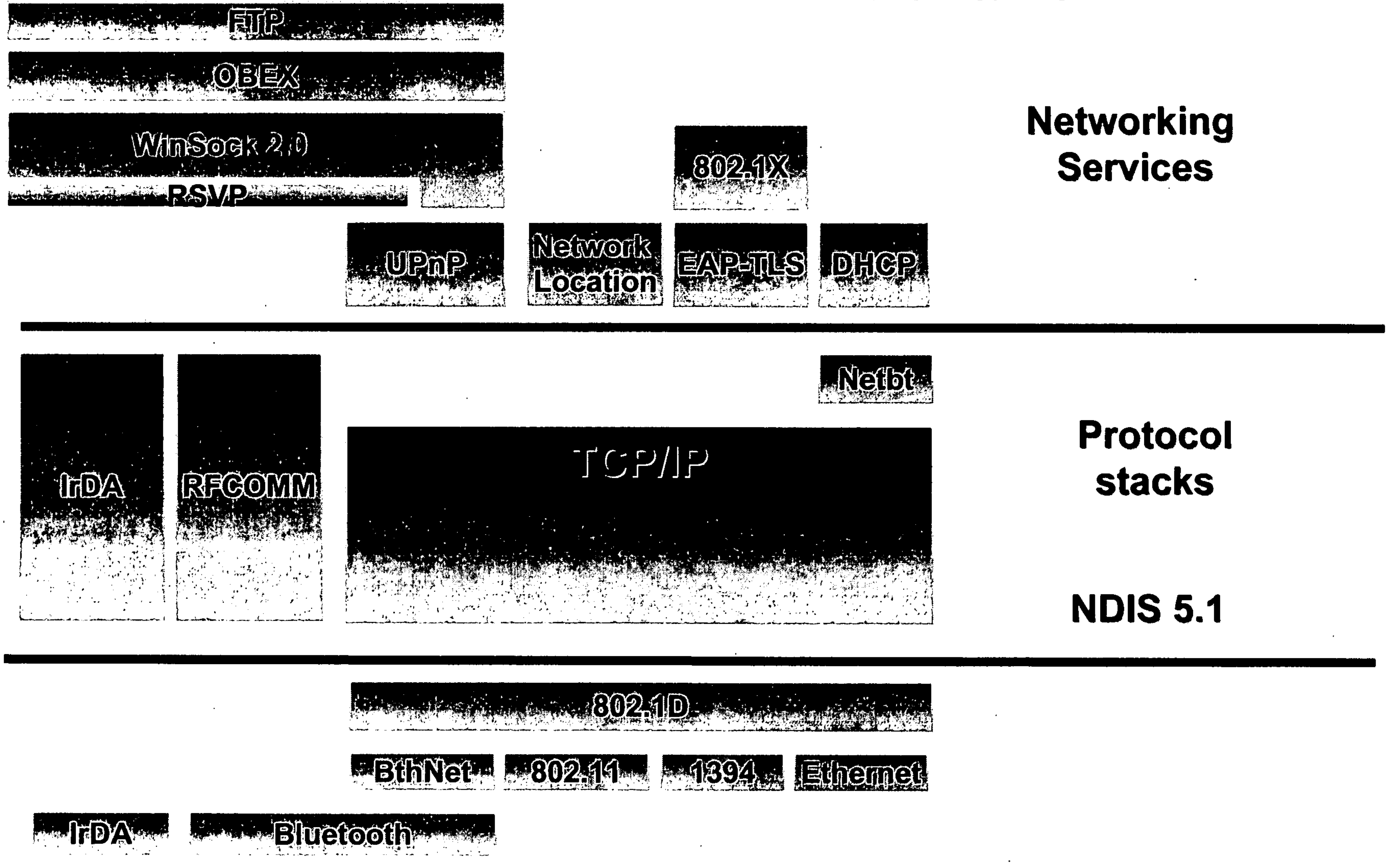
Microsoft® QoS Components



802.11 QoS

- 802.1p support
  - Priority tagging of Ethernet frames
- 802.11 NIC driver
  - Use NDIS priority field to prioritize access from client to wireless network
  - Add 802.1p header for wired network
- Access point prioritizes access from wired network to client based on 802.1p
- Subnetwork bandwidth manager in access point for admission control

Adhoc Architecture



FTP

OBEX

WinSock 2.0

RSVP

802.1X

UPnP

Network Location

EAP-TLS

DHCP

Networking Services

Netbt

IrDA

RFCOMM

TCP/IP

Protocol stacks

NDIS 5.1

802.1D

BthNet

802.11

1394

Ethernet

IrDA

Bluetooth

No Network Infrastructure

- Address assignment
  - APIPA when no DHCP server
  - ICS contains DHCP server for adhoc home network
- Name Resolution
  - NetBT broadcast for adhoc name resolution
  - ICS contains DNS proxy and DDNS support for the adhoc home network
- Service Discovery Protocols
  - SSDP protocol enables UPnP discovery
  - SDP protocol enables Bluetooth wireless technology discovery
  - IrLAP protocol enables IrDA discovery

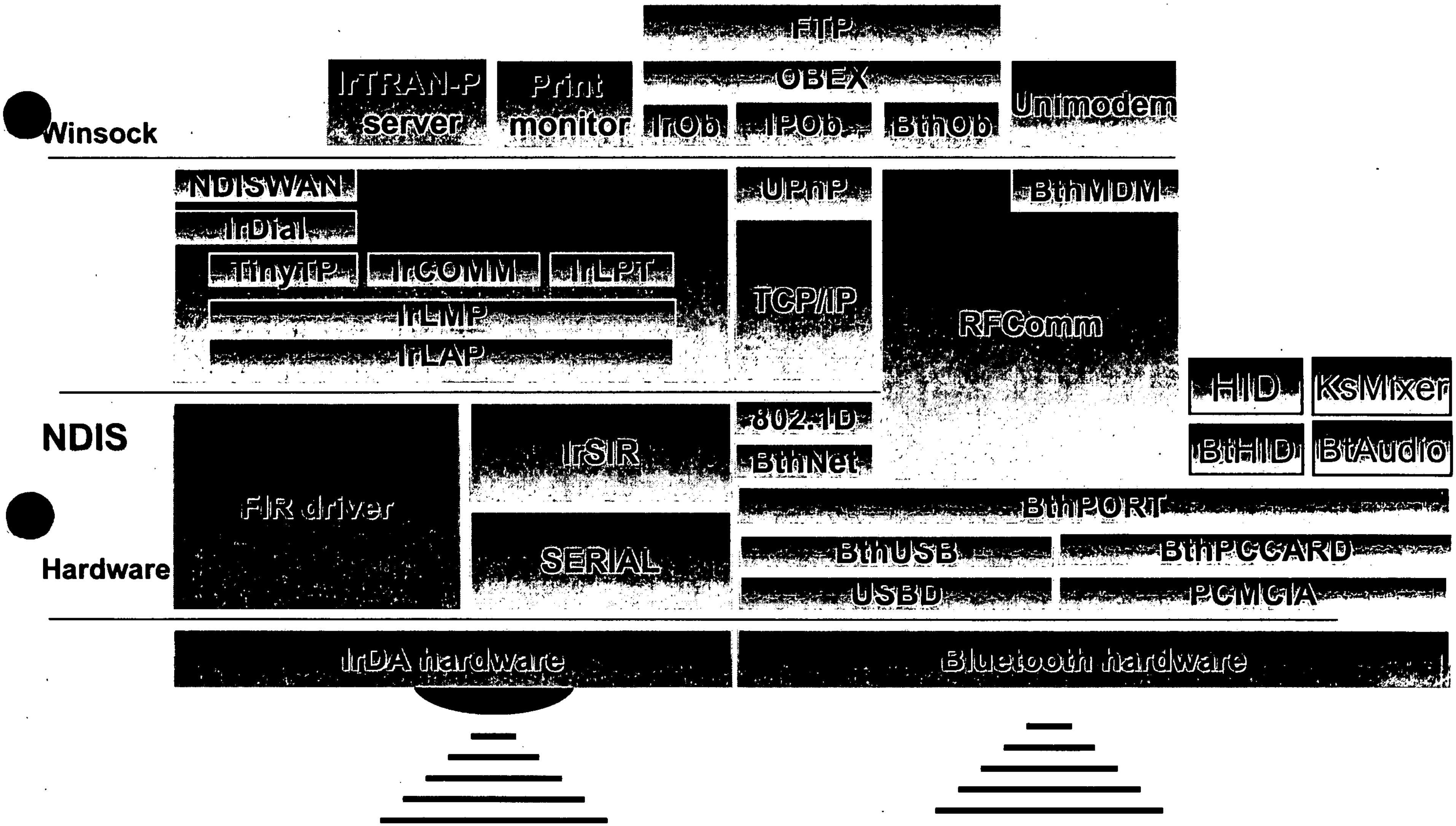
Temporary Networks

- Wireless allows for networks to be setup easily
- Interconnections not organized
  - Multiple interconnections to destinations
  - Loops in the network
- L2 Spanning tree
  - Self organizing networks
  - Removes loops

Ad Hoc Ethernet Networks

- Ethernet hubs
- Ethernet cross-over cables
- 1394
- Host to Host USB cables
- 802.11 can form adhoc mode
  - Automatically switch to adhoc mode when no access points in range
- Bluetooth wireless technology
- IrDA

IrDA/Bluetooth Architecture



IrDA Applications

- File transfer
  - Integrated into shell
- Image exchange from camera
- Dial-up networking via cellphone
- Printing
- Synchronization
  - ActiveSync®

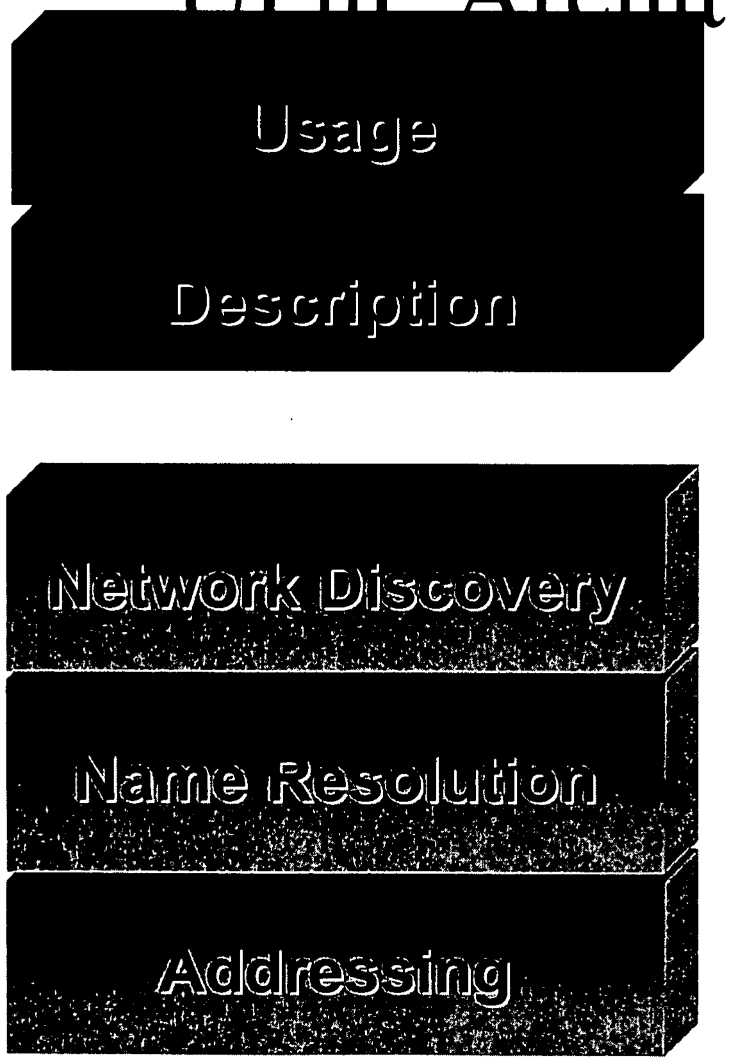
Bluetooth Applications

- Subset of IrDA
- File transfer
  - Integrated into IrDA ftp transfer
- Dial-up Networking via cellphone
- IR and Bluetooth applications are tied to particular media
  - Do not inter-operate

Ad Hoc Applications

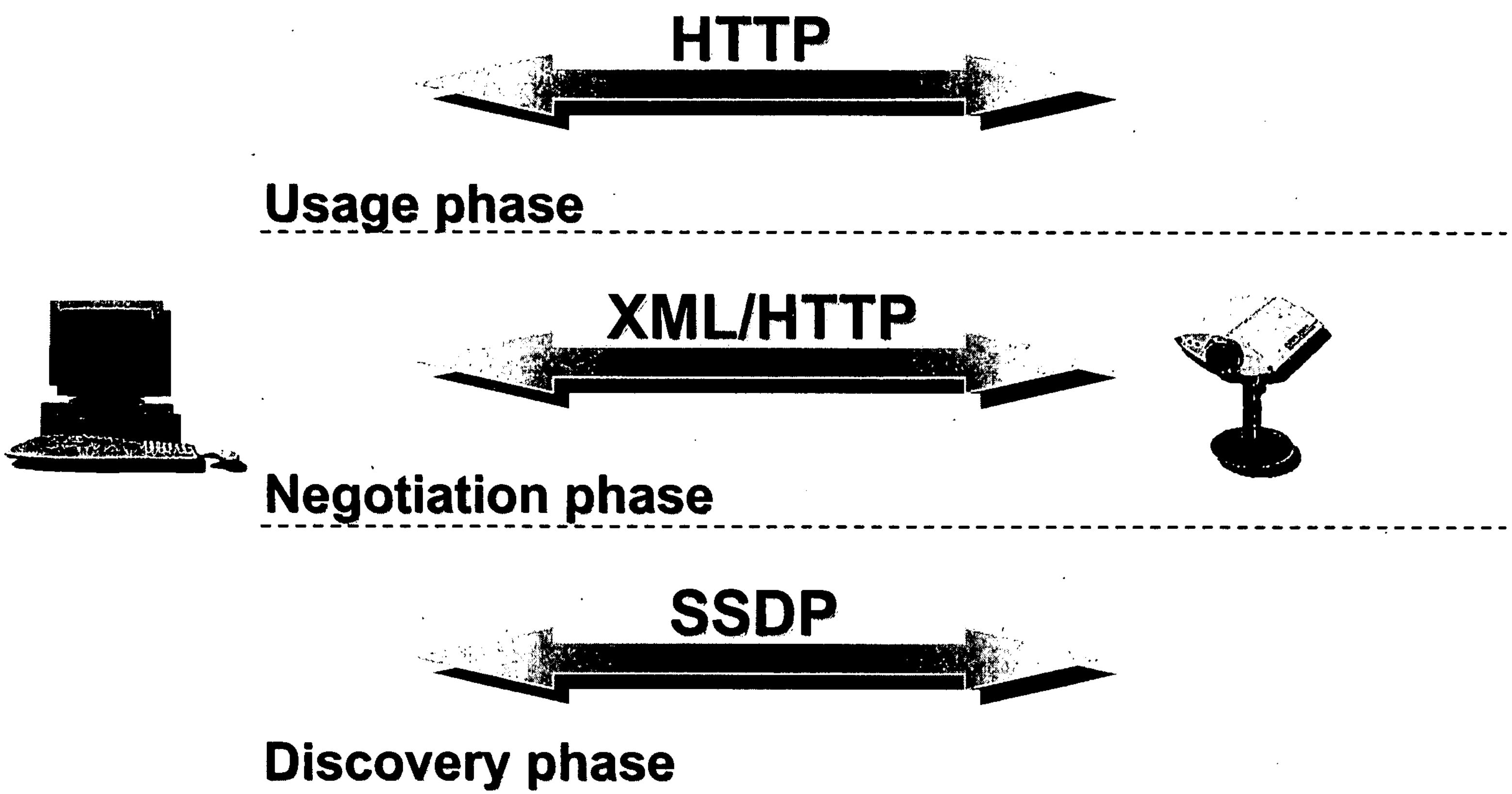
- UPnP is the integration point for ad hoc applications
- UPnP applications and services are available over any IP network
  - Ethernet, Wireless LAN, 1394, etc.

UPnP Architecture Reference



- Description/usage
  - Standardized protocols
  - Standardized XML descriptions
- Simple discovery
  - Locate devices/services on-the-fly
  - Standards-based

How It Works



HTTP

Usage phase

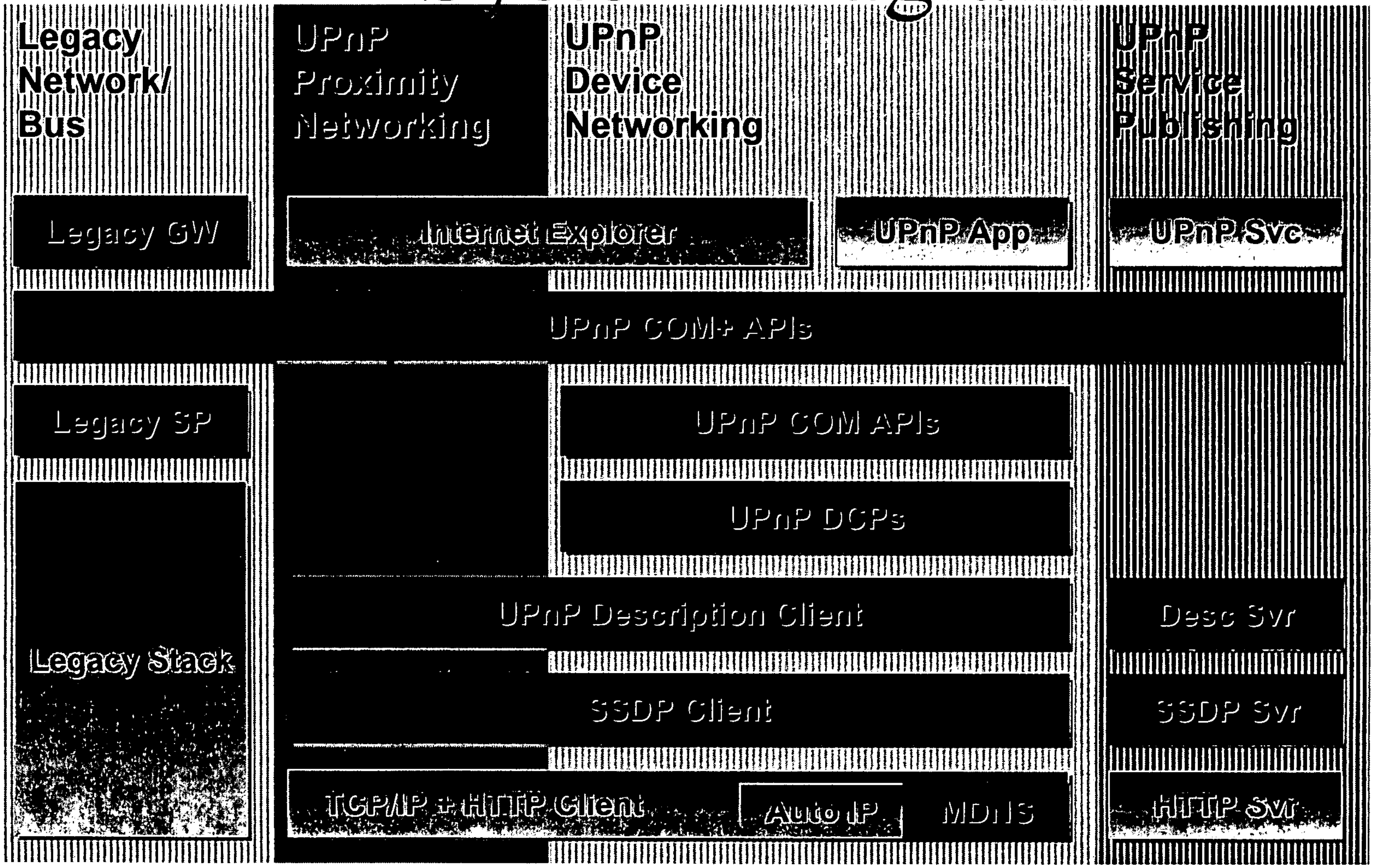
XML/HTTP

Negotiation phase

SSDP

Discovery phase

System Diagram



Legacy Network/ Bus

UPnP Proximity Networking

UPnP Device Networking

UPnP Service Publishing

Legacy GW

Internet Explorer

UPnP App

UPnP Svc

UPnP COM+ APIs

Legacy SP

UPnP COM APIs

UPnP DCPs

Legacy Stack

UPnP Description Client

Desc Svr

SSDP Client

SSDP Svr

TCP/IP + HTTP Client

Auto IP

MDNS

HTTP Svr

Wireless Performance

- TCP has many features optimized for wireless in Windows 2000
  - Improved RTT estimate
  - Improved window sizes
  - Fast retransmit
  - Select acknowledgement
  - Acknowledge packets
  - Improved time-out initiation
    - Very important for wireless losses
    - Cannot be used over the serial port
    - Use Remote NDIS
      - Over USB, IEEE 1394, Bluetooth wireless technology

WAP

- WAP was designed to remove some issues with TCP on long thin links
  - Remove 3 way handshake
    - Proposals to add data on the SYN and SYN-ACK
    - Reduces DOS protection
- Remove IP layer for some media
  - Not removed for GPRS
- Data compression
  - GPRS supports TCP/IP header and user data compression
  - Recommend GPRS systems support protocol header and user data compression
- WML is for small screens
  - E.g. a few lines

Summary – Wireless Is Here

- Bandwidth is growing
- Always connected wireless
- Enables new scenarios
  - Driving new applications
- Security a major issue with wireless
  - 802.1X allows integration into Windows user security system
- UPnP is the framework for adhoc applications

Call To Action

- Mobility
  - – Mediasense is required for roaming support
    - Any wireless device must generate mediasense
- Implement 802.1X in network edge devices
  - – Switches, access points, etc.
- Adhoc services and applications
  - – Implement using UPnP
  - – Do not limit your applications to a particular wireless media

For More Information

- Bluetooth wireless technology
  - [illegible]
- IrDA
  - [illegible]
- UPnP
  - [illegible]
  - [illegible]
- 802.11
  - QoS whitepaper
  - Security whitepaper
  - NIC requirements whitepaper

For More Information

- RNDIS
  - WinHec driver talk
  - [illegible]
- TCP/IP
  - Whitepaper
  - [illegible]

For More Information

- IEEE 802.1X
  - [illegible]
- RADIUS
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
- EAP
  - [illegible]
  - [illegible]

1 Windows Wireless Architecture

Tim Moore
Lead Program Manager
Windows Networking
Microsoft Corporation

2 Agenda

- Wireless trends
  - WAN, LAN, PAN
- Scenarios
  - Adhoc, home, small business
  - Enterprise, ISP
- Wireless architecture
- Summary
- Call to action
- More information

3 Wireless Trends

- IP networks
- Always connected
- Increased bandwidth
- Convenience
- Moving from vertical market to horizontal markets
- Moving from proprietary to standards based
- Proliferation of smart devices
- New scenarios enabled
- Outsourcing
- Adhoc networks

4 Information Anytime, Anywhere
Connecting Everything

5 Data Speeds Today

Network	Speed*	Type of Data
American Mobile ARDIS	19.2/4.8 Kbps	Packet
BellSouth Wireless Data	8 Kbps	Packet
Cellular (Analog)	9.6/4.8 Kbps	Circuit-Switched
CDPD	19.2 Kbps	Packet
CDMA	14.4 Kbps	Circuit-Switched
Nextel	9.6 Kbps	Circuit-switched
GSM	9.6 Kbps	Circuit-Switched
Metricom	28.8 Kbps	Packet as Dial-up
TDMA**	One-Way SMS Only	None

*Typical data throughput speed is usually 50% of gross speed

**TDMA systems do not support data in the U.S. at this time

6 Wide-Area Wireless

7 Local-Area Wireless

8 Personal Area Wireless

9 Personal Area Wireless

- IrDA
  - Around since 1994
  - Available on every PC and lots of devices
    - >20 million existing IrDA devices
    - Camera, PDAs, cellphones, printers, keyboards
- Exploding market fueled by Bluetooth momentum
  - Bluetooth wireless technology is a defacto standard
  - Proliferation of smart devices, convenience of cable replacement, and new usage scenarios

10 Scenarios

- Adhoc
- Home
- Small business
- Enterprise
- ISP

11 Ad Hoc Networks

12 A Connected Home

13 A Connected Small Office

14 Enterprise

- Information at your fingertips
  - At meetings, in the office, on the road
  - Reliable, secure, multimedia LAN

15 Enterprise

- End-user can access the enterprise wireless network transparently over a secure connection
  - The network administrator has control over which users have access to the enterprise wireless LAN
- Enterprise can offer its employees access via ISPs which outsource their authentication to the enterprise
  - End-user has IP connectivity as soon as a CDPD or a GPRS modem is plugged in
  - Make cellphones an always connected Internet access point using GPRS

- End-User can use Netmeeting with wireless LAN, when out of range of LAN can continue to conference via IP connected cellphone

16 An ISP Connected Public Space

- Discovery of proximity services (flight schedules at airport, mall directories, ...)

17 ISP

- Need mixed technologies
  - Higher speed in hot spots, e.g., 802.11
- Need authentication so ISPs can charge
- Allow ISPs to integrate into existing Radius systems
  - Allows ISP roaming agreements
    - Same as outsource dial
- Need to be able to provision unauthenticated users

18 Wireless Architecture

- “Just works”
- Always connected
- Unified transport: IP
- Mobility
- Unified security model
- Adhoc
- QoS
- Performance

19 Wireless Architecture

20 Just Works

- No configuration
  - Especially when roaming
- CDPD
  - Configure Network Equipment Identifier
- 802.11
  - Configure network name and security keys
    - Per location
- Bluetooth wireless technology
  - Configure PIN numbers
    - Per device

21 802.11 Configuration

- Current 802.11 networks need to be configured with name of the network
  - Roaming between multiple networks difficult especially when security is implemented
- Automatically find a wireless network
  - If Access point is beaconing network name, attempt to use that network
  - If no infrastructure available then switch to adhoc mode

22 Always Connected

- Permanent IP connectivity should not use dial-up model

        - A CDPD card should appears as a LAN card
        - A GPRS, EDGE or 3G card or cellphone should appear as a LAN card
            - GPRS Terminal Type Recommendations
                - Cellphone needs to be Type A (voice and packet)
                - PC-Card can be Type C (packet only)
    - Implement an NDIS driver or use Remote NDIS
        - Remote NDIS over Bluetooth connections

23 Remote NDIS

- Remote NDIS enables a bus-agnostic connection to devices that provide network access
- Remote NDIS is both a driver architecture and a command language

24 Unified Transport: IP

- All other media except Bluetooth wireless technology support always connected IP
- Ethernet over point-to-point Bluetooth connections
    - L2 bridge gives an adhoc L2 network
- Adhoc applications use UPnP over IP
- Expect large numbers of wireless connected devices
    - Move to IPv6 for addresses

25 Mobility

- Applications should not rely on having a network available all the time
    - Network connection can disappear at anytime
    - Applications should reconnect automatically if the network appears
- Clients hold state about the network
    - IP address
    - Routes
- Networks hold state about the client
    - Multicast distribution
    - Quality of service
    - Secure access
    - Machine name to IP address mapping
- How to detect when this state is out of date
- Applications also hold state about the network
    - TCP connections
    - E.g. Proxies, firewalls, etc.

26 Mobility

- Detect roaming
    - Mediasense detects working/non-working interfaces

    - Mediasense detects interfaces changing their network connection
- IP address
    - Mediasense triggers a DHCP renew; If renew fails, DHCP gets a new IP address .
    - DHCP updates DNS when an address changes
    - TCP/IP removes IP addresses if NIC not connected
    - Mobile IP allows IP address to stay the same when roaming

27 Mobile IP

- Mobile IP keeps the application IP address the same
    - IPv4 has two options
        - Change the network interface address to a local IP address
        - Use an ARP proxy to keep the same IP address
    - IPv6 only has first option
- Mobile IP Issues
    - How to route efficiently
        - IPv6 fixes this issue
    - Firewall traversal
    - Time to get a local address
        - Doesn't allow Voice over IP roaming
- Doesn't address any of the other issues with multicast, QoS, security, applications
- GPRS and 3G have network layer mobility
- No plans to support Mobile IP until IPv6

28 Mobility

- Multicast
    - Mediasense triggers IGMP refresh on roaming
- QoS
    - Mediasense triggers RSVP refresh on roaming
- Routes
    - Mediasense triggers router detect (IRDP) on roaming
    - Default interface metrics should depend interface speed
    - Routes to no longer existing interface addresses are removed
- Security
    - Mediasense triggers network authentication refresh
- Applications
    - Need to retry connections on connection failure and mediasense
    - Configurations based on network location

29 Network Location API

- Network location is a hint to the application of the network the machine is connected to
- Accessible via Winsock API

    - Query for the connected networks
        - WSALookupServiceBegin
        - WSALookupServiceNext
        - WSALookupServiceEnd
    - Request for notification when the connected networks changes
        - WSANSIoctl (,SIO_NSP_NOTIFY_CHANGE,…)
- Applications that need configuration per network should use this API
    - E.g., application proxies

30 Security

- Secure access to resources in the network
    - This is Windows login
- Secure transfer of data over the network
    - This is IPSec
    - Integrated into Windows credentials using PKI and Kerberos
- Secure access to the network
    - This is available for RAS and VPNs
    - Integrated into Windows credentials using PKI (EAP) and Radius
    - Supports roaming of identities
- No secure access to LAN networks
    - Very important for Wireless

31 Wireless Security Issues

- User loses wireless NIC, doesn't report it
    - Without user authentication, Intranet now accessible by attackers
    - Without centralized accounting and auditing, no means to detect unusual activity
        - Users who don't log on for periods of time
        - Users who transfer too much data, stay on too long
        - Multiple simultaneous logins
        - Logins from the "wrong" machine account
    - With global keys, large scale re-keying required

32 Wireless Deployment Issues

- User administration
    - Integration with existing user administration tools required (RADIUS, LDAP-based directories)
        - Create a Windows group for wireless
        - Any user or machine who is a member of the group has wireless access
    - Identification via User-Name easier to administer than MAC address identification
    - Usage accounting and auditing desirable
- Key management

    - Static keys difficult to manage on clients, access points
    - Proprietary key management solutions require separate user databases

33 802.1X Topology

34 IEEE 802.1X

- Enables interoperable user identification, centralized authentication, key management
    - Leverages existing standards: EAP, RADIUS
    - Compatible with existing roaming technologies, enabling use in hotels and public places
- User-based identification
    - Identification based on Network Access Identifier (RFC 2486) enables support for roaming access in public spaces (RFC 2607)
- Dynamic key management
- Centralized user administration
    - Support for RADIUS (RFC 2138, 2139) enables centralized authentication, authorization and accounting
    - RADIUS/EAP (draft-ietf-radius-ext-07.txt) enables encapsulation of EAP packets within RADIUS
- Supported on Ethernet, Token Ring and 802.11

35 Extensible Authentication Protocol

- Used by PPP for RAS and VPN
- Allows support for a number of authentication mechanisms
    - EAP designed to allow additional authentication methods to be deployed with no changes to the access point or client NIC
    - RFC 2284 includes support for password authentication (EAP-MD5), One-Time Passwords (OTP)
    - Windows 2000 supports smartcard authentication (RFC 2716) and Security Dynamics
- Radius server used for authentication and authorization
    - Integrated into Active Directory™ users and groups
    - Supports cross authentication for roaming

36 802.1X On 802.11

37 Outsourced Remote Access

- User sends authentication request to ISP
- ISP Delegates authentication to Corporation
- Corporation checks Active Directory
- Single point of administration

38 Provisioning Public Internet

39 Bluetooth Security

- To connect to a Bluetooth device requires its PIN
- PIN is per device not per service
    - Great for personal single function devices
    - E.g., protect cellphone from being dialed

- Problem for adhoc devices/applications
  - Require PIN for each device
  - Obtain access to all services on device
- Need security at a higher level and no PIN
  - Adhoc FTP user intervention required so why need a pin?
  - Adhoc PAN do not want a PIN otherwise cannot setup roaming PANs
  - Business card exchange should be push to a destination

40 GPRS Security

- GPRS uses GSM Authentication
- Authentication is between the mobile station and the network
  - Need authentication between PC and the Bluetooth mobile station
    - Bluetooth PIN

41 Microsoft® QoS Components

42 802.11 QoS

- 802.1p support
  - Priority tagging of Ethernet frames
- 802.11 NIC driver
  - Use NDIS priority field to prioritize access from client to wireless network
  - Add 802.1p header for wired network
- Access point prioritizes access from wired network to client based on 802.1p
- Subnetwork bandwidth manager in access point for admission control

43 Adhoc Architecture

44 No Network Infrastructure

- Address assignment
  - APIPA when no DHCP server
  - ICS contains DHCP server for adhoc home network
- Name Resolution
  - NetBT broadcast for adhoc name resolution
  - ICS contains DNS proxy and DDNS support for the adhoc home network
- Service Discovery Protocols
  - SSDP protocol enables UPnP discovery
  - SDP protocol enables Bluetooth wireless technology discovery
  - IrLAP protocol enables IrDA discovery

45 Temporary Networks

- Wireless allows for networks to be setup easily
- Interconnections not organized
  - Multiple interconnections to destinations
  - Loops in the network
- L2 Spanning tree
  - Self organizing networks

    - Removes loops

46 Ad Hoc Ethernet Networks

- Ethernet hubs
- Ethernet cross-over cables
- 1394
- Host to Host USB cables
- 802.11 can form adhoc mode
    - Automatically switch to adhoc mode when no access points in range
- Bluetooth wireless technology
- IrDA

47 IrDA/Bluetooth Architecture

48 IrDA Applications

- File transfer
    - Integrated into shell
- Image exchange from camera
- Dial-up networking via cellphone
- Printing
- Synchronization
    - ActiveSync®

49 Bluetooth Applications

- Subset of IrDA
- File transfer
    - Integrated into IrDA ftp transfer
- Dial-up Networking via cellphone
- IR and Bluetooth applications are tied to particular media
    - Do not inter-operate

50 Ad Hoc Applications

- UPnP is the integration point for ad hoc applications
- UPnP applications and services are available over any IP network
    - Ethernet, Wireless LAN, 1394, etc.

51 UPnP Architecture Reference

- Description/usage
    - Standardized protocols
    - Standardized XML descriptions
- Simple discovery
    - Locate devices/services on-the-fly
    - Standards-based

52 How It Works

53 System Diagram

54 Wireless Performance

- TCP has many features optimized for wireless in Windows 2000
  - Improved RTT estimate
  - Improved window sizes
  - Fast retransmit
  - Select acknowledgement
  - Acknowledge packets
  - Improved time-out initiation
    - Very important for wireless losses
    - Cannot be used over the serial port
    - Use Remote NDIS
      - Over USB, IEEE 1394, Bluetooth wireless technology

55 WAP

- WAP was designed to remove some issues with TCP on long thin links
  - Remove 3 way handshake
    - Proposals to add data on the SYN and SYN-ACK
    - Reduces DOS protection
- Remove IP layer for some media
  - Not removed for GPRS
- Data compression
  - GPRS supports TCP/IP header and user data compression
  - Recommend GPRS systems support protocol header and user data compression
- WML is for small screens
  - E.g., a few lines

56 Summary – Wireless Is Here

- Bandwidth is growing
- Always connected wireless
- Enables new scenarios
  - Driving new applications
- Security a major issue with wireless
  - 802.1X allows integration into Windows user security system
- UPnP is the framework for adhoc applications

57 Call To Action

- Mobility
  - Mediasense is required for roaming support
    - Any wireless device must generate mediasense
- Implement 802.1X in network edge devices
  - Switches, access points, etc.
- Adhoc services and applications

- Implement using UPnP
- Do not limit your applications to a particular wireless media

58 For More Information

- Bluetooth wireless technology
  - http://www.bluetooth.com
- IrDA
  - http://www.irda.org
- UPnP
  - http://www.upnp.org
  - http://www.microsoft.com/hwdev/upnp
- 802.11
  - QoS whitepaper
  - Security whitepaper
  - NIC requirements whitepaper

59 For More Information

- RNDIS
  - WinHec driver talk
  - http://www.microsoft.com/hwdev/network
- TCP/IP
  - Whitepaper
  - http://www.microsoft.com/windows2000/library/howitworks/communications/networkbasics/tcpip_implement.asp

60 For More Information

- IEEE 802.1X
  - http://grouper.ieee.org/groups/802/1/pages/802.1x.html
- RADIUS
  - http://www.ietf.org/rfc/rfc2138.txt
  - http://www.ietf.org/rfc/rfc2139.txt
  - http://www.ietf.org/rfc/rfc2548.txt
  - http://www.ietf.org/internet-drafts/draft-ietf-radius-radius-v2-06.txt
  - http://www.ietf.org/internet-drafts/draft-ietf-radius-accounting-v2-05.txt
  - http://www.ietf.org/internet-drafts/draft-ietf-radius-ext-07.txt
  - http://www.ietf.org/internet-drafts/draft-ietf-radius-tunnel-auth-09.txt
  - http://www.ietf.org/internet-drafts/draft-ietf-radius-tunnel-acct-05.txt
- EAP
  - http://www.ietf.org/rfc/rfc2284.txt
  - http://www.ietf.org/rfc/rfc2716.txt